The Financial Services Information Sharing and Analysis Center – FS-ISAC

Article Submitted by Ted Hansen, FS-ISAC

Information – Timely, Accurate, Authoritative, and possibly Critical to your institution's well being. It is something every organization needs and when it comes to understanding the cyber and physical threat environment, the impact can not only be costly in terms of your safety and your infrastructure, it can ruin your reputation in an instant.

Recognizing this reality, the Government of the United States sanctioned and established Information Sharing and Analysis Centers for several "critical infrastructures," among them Financial Services. 1998's Presidential Directive 63 (later updated by 2003's Homeland Security Presidential Directive 7) led to the creation of the FS-ISAC, on the eve of the Y2K event and in response to the growth, complexity, and great potential of the Internet, for both good and evil. Other critical infrastructures were defined, such as communications, electricity, transportation, and emergency services; in all there are now 17. Each of these ISACs enjoys a special relationship with branches of the Government, and in the case of Financial Services, ours is with the Department of Treasury. Additional lines of communication have been established with other agencies, especially the Department of Homeland Security, to complement existing traditional relationships with the regulatory community, Secret Service, FBI, the Federal Reserve, and more recently the various state agencies.

From this base in information security, the FS-ISAC has grown, in terms of members (now in excess of 4300) and in its mission. The FS-ISAC now reaches beyond cyber-security to include physical security, an incident notification system (Critical Infrastructure Notification System, or CINS), anonymous information sharing, member surveys, regular and emergency conference calls, and more. Originally funded with a grant from the Department of Treasury, FS-ISAC is now a member owned not-for-profit with a Board of Directors and Advisors drawn from its membership.

If you are a financial services firm, or serve the sector, you have the responsibility for doing your part to help protect our country's banking and finance critical infrastructure. Treasury, DHS, the U.S. Secret Service, and the Financial Services Sector Coordinating Council (www.fsscc.org) recommend membership in the FS-ISAC. The private sector owns in excess of 90% of the critical infrastructure of the U.S. so it is in our best interest to control our destiny as much as possible. Further, the goal of the Department of Treasury is to have ONE place where they can turn and, if they issued information or a

directive, connect with the entire financial sector. That vehicle to reach all those financial services organizations is the FS-ISAC.

As such, FS-ISAC's goal is to get 98% of the entire industry as direct participants. Both Treasury and the Department of Homeland Security use the FS-ISAC to disseminate critical information to the financial services sector in times of crisis. Federal Regulators list participation in and usage of ISAC information as something they will be reviewing in their examination process. (See the FFIEC's Information Security Handbook published in July of 2006, Security Monitoring Section, Security Incidents Subsection under Analysis and Response).

But beyond the regulatory imperative, there are additional reasons you should seriously consider membership. The FS-ISAC acts as your radar – you will see many blips on the screen that may or may not impact your organization, but eventually there will be something of significant importance to you. Here are actual examples:

- two incidents where internet security providers made us aware of keylogging files which contained bank account information with user names and passwords that were shut down before the accounts were compromise;
- the discovery by our Security Operations Center of a particularly nasty Trojan (Torpig) imbedded on the web sites of our members that could have launched and captured customer information through a "man in the middle" scheme;
- important information, such as, according to the Anti-phishing Working Group, 93.8% of the attacks that were launched in November of 2007 were against financial institutions, or, according to the IBM Internet Security Systems X-Force® 2007 Trend Statistics, of the top 20 companies targeted by phishing in 2007, 19 are in the banking industry, and one conducts recruiting.
- a thorough analysis of a recent number of spear phishing (individually targeted phishing attacks) that were initiated to encourage small businesses to provide account information about their bank-based treasury management systems, allowing perpetrators to compromise those systems and steal company funds. In a conference call, there were several institutions that had experienced these attacks and were able to share their experiences with others.

Individuals and organizations with bad intent will continue to target financial institutions, and if they have a hard time compromising the larger, more sophisticated institution, they will move to smaller ones, as they did recently when an international gang of cyber criminals hacked into a Texas bank's records. They stole account numbers, created new PINs, fabricated debit cards, then withdrew cash from ATMs in Eastern Europe, including Russia and Ukraine, as well as in Britain, Canada and New York.

FS-ISAC's members include the entire expanse of financial institutions and the organizations that support them. Our member levels reflected that diversity, and the cost to join ranges from hundreds of dollars to many thousands. Larger financial institutions with diverse security needs and large staffs typically join at the higher membership levels. We recently revamped our entry member levels to recognize that the person with security and business continuity responsibility at smaller, community-based organizations may also wear other hats – indeed we typically find auditors, CFO's, bank operation managers, the occasional CEO, in short almost anyone, as the key point of contact in these companies.

For as little as $200, a financial institution (with less than $1 billion in assets) can become a basic member and designate a key individual to receive all the e mails, alerts, participation in CINS, access to our portal, in short all of the services they typically require to meet their needs. Other institutions will find our Core membership offering at $750 still a bargain for their requirements. Core membership allows up to four user-ids per institution. The larger financial institutions in Georgia are already among our best and most supportive members at the higher levels of membership

Recently you may have read an article here about Georgia FIRST, a regional recovery coalition being established to represent the financial services community in the event of an emergency. Indeed, you were invited to contact either me or Rick Kelly of Synovus to find out more information and join us. FS-ISAC is a strong supporter of these entities. Our staff in the DC area participates in their coalition and I am participating here in Georgia. Georgia First is the local, on-the-ground tactical organization that will be on the front lines during a tragedy striking our state. FS-ISAC looks forward to supporting Georgia FIRST and the financial institutions that join with complementary services and information.

Please visit the FS-ISAC web site at www.fsisac.com to find out more, and do not hesitate to contact Ted Hansen, Deputy Director, at 770-664-4207 or thansen@fsisac.us, if you have any questions.